SAMPLE

Quantum Cryptography

Unbreakable Codes

Aira Astralis

Free sample: Introduction & Chapter 1

putrabooks.github.io

Buy the full book:

Carousell carousell.sg/p/quantum-cryptography-ebook-pdf-1467816874

ElevenReader

Ko-fi

Payhip

Gumroad

Contents

Introduction

Chapter 1: The Discovery of Quantum Cryptography

Chapter 2: Understanding Quantum Cryptography

Chapter 3: Key Characteristics of Quantum Cryptography

Chapter 4: The Science Behind Quantum Cryptography

Chapter 5: Observation and Measurement of Quantum Cryptography

Chapter 6: Important Features of Quantum Cryptography

Chapter 7: Quantum Cryptography in Context

Chapter 8: Modern Understanding of Quantum Cryptography

Chapter 9: Research and Exploration of Quantum Cryptography

Chapter 10: Challenges and Mysteries of Quantum Cryptography

Chapter 11: Future Directions in Quantum Cryptography Research

Chapter 12: Fun Facts and Trivia About Quantum Cryptography

Chapter 13: Conclusion: The Significance of Quantum Cryptography

Conclusion

This free sample contains the Introduction and Chapter 1. The complete book contains the full contents above.

Introduction

Quantum cryptography is the exploiting of quantum-mechanical properties such as quantum entanglement, measurement disturbance, no-cloning theorem, and the principle of superposition to perform encryption tasks. Quantum encryption plays a crucial role in the secure processing, storage, and transmission of information. One aspect of quantum cryptography is quantum key distribution (QKD), which offers an information-theoretically secure solution to the key-exchange problem. Quantum cryptography allows the completion of cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e., non-quantum) communication.

Furthermore, quantum cryptography affords the authentication of messages, which allows the legitimate parties to prove that the messages were not wiretapped during transmission. Thus, in a cryptographic set-up, it is impossible to copy, with perfect fidelity, the data encrypted in a quantum state. If one attempts to read the encrypted data, the quantum state will be changed due to wave function collapse (no-cloning theorem). This could be used to detect eavesdropping in QKD schemes, or in quantum communication links and networks.

These advantages make quantum cryptography important in the digital age, where devices are increasingly interconnected and cyberattacks have become increasingly sophisticated. Quantum-mechanical properties - more specifically, quantum authentication - are critical components in the advancement of a quantum internet, as they establish robust mechanisms to ensure the long-term privacy and integrity of digital communications and systems. In the early 1970s, Stephen Wiesner, then at Columbia University in New York, introduced the concept of quantum conjugate coding.

His seminal paper titled "Conjugate Coding" was rejected by the IEEE Information Theory Society but was eventually published in 1983 in SIGACT News. In this paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of photons, so that either, but not both, properties may be received and decoded. It was not until Charles H. Bennett, of the IBM's Thomas J.

Watson Research Center, and Gilles Brassard met in 1979 at the 20th IEEE Symposium on the Foundations of Computer Science, held in Puerto Rico, that they discovered how to incorporate Wiesner's findings.

In the quantum setting, they would be particularly useful: Crépeau and Kilian showed that from a commitment and a quantum channel, one can construct

an unconditionally secure protocol for performing so-called oblivious transfer.

Chapter 1: The Discovery of Quantum

Cryptography

Independently, in 1991 Artur Ekert proposed to use Bell's inequalities to achieve secure key distribution. Ekert's protocol for the key distribution, as it was subsequently shown by Dominic Mayers and Andrew Yao, offers device-independent quantum key distribution. Companies that manufacture quantum cryptography systems include MagiQ Technologies, Inc. Cryptography is the strongest link in the chain of data security. However, interested parties cannot assume that cryptographic keys will remain secure indefinitely.

Quantum cryptography has the potential to encrypt data for longer periods than classical cryptography. Using classical cryptography, scientists cannot guarantee encryption beyond approximately 30 years, but some stakeholders could use longer periods of protection. Take, for example, the healthcare industry. As of 2017, 85.9% of office-based physicians are using electronic medical record systems to store and transmit patient data. Under the Health Insurance Portability and Accountability Act, medical records must be kept secret.

Quantum key distribution can protect electronic records for periods of up to 100 years. Also, quantum cryptography has useful applications for governments and militaries as, historically, governments have kept military data secret for periods of over 60 years. There also has been proof that quantum key distribution can travel through a noisy channel over a long distance and be secure. It can be reduced from a noisy quantum scheme to a classical noiseless scheme. This can be solved with classical probability theory.

This process of having consistent protection over a noisy channel can be possible through the implementation of quantum repeaters. Quantum repeaters have the ability to resolve quantum communication errors in an efficient way. Quantum repeaters, which are quantum computers, can be stationed as segments over the noisy channel to ensure the security of communication. Quantum repeaters do this by purifying the segments of the channel before connecting them creating a secure line of communication.

Sub-par quantum repeaters can provide an efficient amount of security through the noisy channel over a long distance. Quantum cryptography is a general subject that covers a broad range of cryptographic practices and protocols. While encryption techniques are widely recognized and understood, a significant challenge remains in the secure distribution of shared keys, often referred to as key establishment or key agreement. Quantum Key Distribution (QKD) aims to address this particular challenge.

Below, we explore various notable methodologies and applications currently

employed in quantum cryptography.

The best-known and developed application of quantum cryptography is QKD, which is the process of using quantum communication to establish a shared key between two parties (Alice and Bob, for example) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. If Eve tries to learn information about the key being established, discrepancies will arise causing Alice and Bob to notice.

Once the key is established, it is then typically used for encrypted communication using classical techniques. For instance, the exchanged key could be used for symmetric cryptography (e.g. The security of quantum key distribution can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something not possible with classical key distribution.

This is usually described as "unconditional security", although there are some minimal assumptions required, including that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other, i.e. Eve should not be able to impersonate Alice or Bob as otherwise a man-in-the-middle attack would be possible. While QKD is secure, its practical application faces some challenges. There are in fact limitations for the key generation rate at increasing transmission distances.

Recent studies have allowed important advancements in this regard.

In 2018, the protocol of twin-field QKD was proposed as a mechanism to overcome the limits of lossy communication. The rate of the twin field protocol was shown to overcome the secret key-agreement capacity of the lossy communication channel, known as repeater-less PLOB bound, at 340 km of optical fiber; its ideal rate surpasses this bound already at 200 km and follows the rate-loss scaling of the higher repeater-assisted secret key- agreement capacity (see figure 1 of and figure 11 of for more details).

The protocol suggests that optimal key rates are achievable on "550 kilometers of standard optical fibre", which is already commonly used in communications today. The theoretical result was confirmed in the first experimental demonstration of QKD beyond the PLOB bound which has been characterized as the first effective quantum repeater. Notable developments in terms of achieving high rates at long distances are the sending-not-sending

(SNS) version of the TF-QKD protocol.

In mistrustful cryptography the participating parties do not trust each other.

For example, Alice and Bob collaborate to perform some computation where both parties enter some private inputs. But Alice does not trust Bob and Bob does not trust Alice. Thus, a secure implementation of a cryptographic task requires that after completing the computation, Alice can be guaranteed that Bob has not cheated and Bob can be guaranteed that Alice has not cheated either.

Examples of tasks in mistrustful cryptography are commitment schemes and secure computations, the latter including the further examples of coin flipping and oblivious transfer. Key distribution does not belong to the area of mistrustful cryptography. Mistrustful quantum cryptography studies the area of mistrustful cryptography using quantum systems.

The goal of position-based quantum cryptography is to use the geographical location of a player as its (only) credential.

The notion of using quantum effects for location verification first appeared in the scientific literature in 2010.

Currently, research is being conducted mainly in Japan and China: e.g. The principle of operation is as follows. Wyner is implemented.

The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs.

End of free sample. The full book is available at putrabooks.github.io

ABOUT THE AUTHOR

Aira Astralis is a science writer specializing in astronomy and space exploration. Her work spans the full breadth of humanity's relationship with the cosmos -- from the earliest naked-eye observations to the engineering marvels of modern space missions.

Her books are built on a foundation of primary sources: peer-reviewed research, mission archives, and direct engagement with the scientific community. She writes for readers who want to understand not just what we know about the universe, but how we came to know it.

She believes that the most important frontier is not out there but in the gap between what scientists discover and what the public understands. Her books exist to close that gap.